

Synopsis on Wireless Ethernet (IEEE 802.11)

James D. Gilsinn

National Institute of Standards & Technology

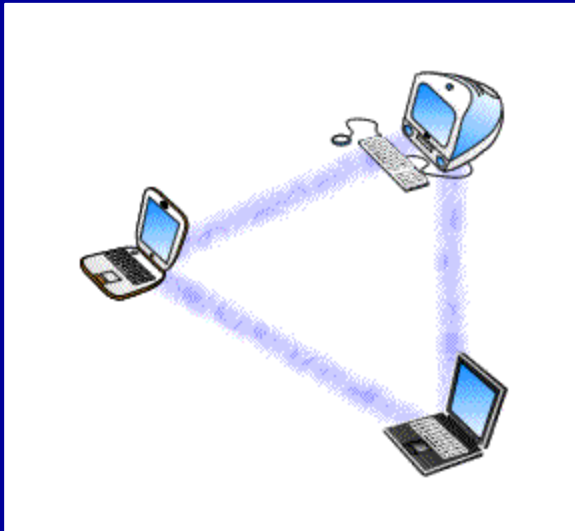
Intelligent Systems Division

james.gilsinn@nist.gov

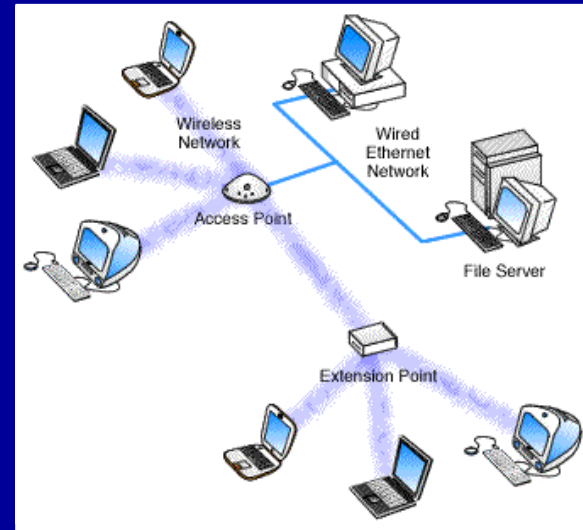
What is IEEE 802.11?

- IEEE 802.11 is an extension of the Ethernet standard (802.3) into wireless communications
- Allows roaming computers to talk to other devices (peer-to-peer) or connect to a wired network (transmitter/receiver)
- IEEE standard allows interoperability between multiple vendor's products

802.11 Network Examples



Peer-to-Peer Network



Transmitter/Receiver
(Wired/Wireless Network)

Pictures from Vicomsoft Web Site, <http://www.vicomsoft.com/>

IEEE 802.11 Specification



- Original specification 1997, revised 1999
- Speed: 1/2 Mbps
- Operating Range: 10-100m inside, 300m outside
- Power Output: 100mW typical
- Frequency Hopping (FHSS), Direct Sequence (DSSS), Infrared (IrDA)
 - Networks are NOT compatible with one another
- Uses 2.4 GHz ISM band (2.402-2.480 GHz)

802.11 Variations



- IEEE 802.11a
 - Speed: 6-54 Mbps
 - Uses 5 GHz ISM band (5.15-5.35 GHz)
 - Standard approved in 1999, but chip-sets and products only just starting to emerge
 - Recently selected by the Dedicated Short Range Communications (DSRC) Vendors' Consortium as the preferred technology to provide the national interoperability for Public Safety based applications

802.11 Variations (cont'd)



- IEEE 802.11b
 - Speed: 5.5/11 Mbps
 - Direct Sequence Spread Spectrum (DSSS) only
 - Backward compatible with 802.11 devices using DSSS
 - Most common implementation of wireless Ethernet
- IEEE P802.11e
 - Make Quality of Service (QoS) enhancements
- IEEE P802.11f
 - Improve the interoperability of Access Points

802.11 Variations (cont'd)



- IEEE P802.11g
 - Develop higher speed extension for 802.11b standard
 - Speed: > 20 Mbps
- IEEE P802.11h
 - Enhance the 802.11 and 802.11a standards to enable regulatory acceptance of 5 GHz products
- IEEE P802.11i
 - Originally part of P802.11e
 - Improve the security and authentication mechanisms

802.11 Variations (cont'd)



MAC	802.11 MAC	802.11e MAC Enhancements - QoS	
		802.11f Access Point Interoperability	
		802.11i Enhanced Security Mechanisms	
PHY	Infrared (IrDA)	802.11 IrDA 1/2 Mbps	
	2.4 GHz (FHSS) Frequency Hopping Spread Spectrum	802.11 FHSS 1/2 Mbps	
	2.4 GHz (DSSS) Direct Sequence Spread Spectrum	802.11 DSSS 1/2 Mbps	
		802.11b 5.5/11 Mbps Extension	802.11g >20 Mbps Extension
	5 GHz (OFDM) Orthogonal Frequency Division Multiplexing	802.11a 6-54 Mbps Extension	802.11h Spectrum Management
			5 GHz Globalization

802.11 Security



- IEEE 802.11 uses Wired Equivalent Privacy (WEP) algorithm to prevent eavesdropping
- WEP algorithm is self-synchronizing
- 64-bit key (40-bit secret code, 24-bit “init” vector)
 - 128-bit keys seem common in production devices
- Data integrity checked with 32-bit cyclical redundancy check (CRC-32)
- Can be implemented in hardware or software

802.11 Security (cont'd)



- Uses the same key to encrypt/decrypt message
 - This is a known security problem
- 64-bit WEP has been cracked!
 - Multiple groups have reported being able to crack the secret code from a 64-bit WEP network in 15 minutes
- It is unclear whether the 128-bit encryption would provide much better security!
- Like wired networks, other precautions may be required to ensure data security

802.11 and Bluetooth



- Tests have shown significant affects of having both IEEE 802.11b and Bluetooth devices in close proximity
 - Good results as long as Bluetooth devices are kept 10m away from the 802.11 Access Point (AP)
 - Worse results when Bluetooth devices are near Station

Summary & References



- 802.11 provides
 - Flexibility
 - Interoperability
 - Upgradability
 - Ease of Use
- Although it has its drawbacks, 802.11 may provide a good extension to industrial Ethernet
- <http://www.ieee.org>
- <http://www.wlana.com>
- <http://www.wirelessethernet.org>
- <http://www.itsa.org>
- <http://www.zdnet.com>
- <http://www.internetnews.com>
- <http://www.oreillynet.com>
- <http://www.vicomsoft.com>
- <http://www.atheros.com>
- <http://www.proxim.com>
- <http://www.cisco.com>